

UNITED STATES OF AMERICA)

v.)

Manning, Bradley E.)
PFC, U.S. Army,)
HHC, U.S. Army Garrison,)
Joint Base Myer-Henderson Hall)
Fort Myer, Virginia 22211)

**STIPULATION OF
EXPECTED TESTIMONY**

SA Kirk Ellis

7 June 2013

It is hereby agreed by the Accused, Defense Counsel, and Trial Counsel, that if SA Kirk Ellis were present to testify during the merits and pre-sentencing phases of this court-martial, he would testify substantially as follows:

1. I am currently a Special Agent (SA) criminal investigator and certified digital forensic examiner for United States Army Criminal Investigation Command (CID). I am assigned to the Rock Island Fraud Resident Agency within the Major Procurement Fraud Unit and am currently deployed to Afghanistan. In this position, I investigate fraud cases as a case agent. When in the United States, I also provide forensic examination services to our local field offices. I have held this position for about one year. Previously, I worked at CID's Computer Crimes Investigative Unit (CCIU) as a Computer Crime Program Manager at Fort Belvoir, Virginia and Marine Corps Base-Quantico, Virginia. I have also worked as a case agent with CCIU. I have been a civilian SA with CID since 2008. Before that, I was an active duty CID agent for three years at Fort Bragg, North Carolina.

2. I have substantial training to qualify me for my position. I have attended several courses run by the Defense Cyber Investigations Training Academy (DCITA) in Linthicum, Maryland. I have used the EnCase forensic tool on multiple occasions in my line of work. I am also a Department of Defense Certified Computer Crime Investigator. I have a bachelor's degree in multi-disciplinary studies with a focus on business and criminal justice from Liberty University in Lynchburg, Virginia. I have worked more than a dozen fraud cases, approximately a dozen cases for CCIU, and about fifty to sixty cases as an active duty CID SA.


3. I first became involved in this case when I was a case agent with CCIU. Throughout the course of this investigation, I worked with several other SAs on the investigation team, including SA Bowen, SA Wilbur, SA Edwards, SA Ames, and SA Mander. Primarily, my role on the investigative team was to assist with witness questioning and with electronic data collection. Specifically, SA Bowen and I collected the Department of State (DoS) server logs on 15 June 2010. After coordinating with Mr. Albert "John" Janek at the DoS for authorization, we collected the logs from a server room in the Harry S. Truman Building of the DoS in Washington, DC. We were interested in collecting the DoS server logs so we could see users that had accessed the servers, and what files were specifically accessed. In this instance, we collected, or copied, the logs from January 2009 to June 2009, and from 30 April 2010 to 15 June 2010. We were not able to collect DoS server log files between July 2009 and 30 April 2010 based on an electronic recording gap. The files that were copied were placed in ".zip" files and named "logs.zip" and "newlogs.zip." I collected these log files in accordance with the training I have received. The DoS gave me a host computer that could access the logs between

their firewalls and collected the files on a clean USB removable drive ("thumb drive"). It was my practice to wipe and format a thumb drive prior to collection. Wiping is more than just deleting; it means forensically removing all information from a drive. It ensures the device is completely empty of all types of data. Mr. Janek first possessed the thumb drive, and then signed it over to me when I finished collecting the files from the host computer.

4. After Mr. Janek signed the thumb drive over to me, I brought the thumb drive back to CID. I created an image of the information using EnCase. I imaged these items of evidence so that the data on the device can be forensically examined without exposing the actual collected contents to examination. The image I created was verified by hash value match. I encountered no errors while conducting the imaging of the evidence at issue in this case. Once I verified that the hash values matched, I saved the EnCase image on a DVD so that it could be examined and logged it as evidence. I know it was clean and appropriate for evidence collection for two reasons. First, it was the same type of DVD our office uses to collect evidence in our standard digital evidence collection practices. Second, it was new and factory-made. I know the data I put onto it had been unaltered because the hash value of the logs collected onto the clean thumb drive matched the hash value of the logs after I saved them to the DVD. The DVD was marked "0028-10-cid221-10117 Dept of State Server Logs, 199.56.188.73". I used a DA Form 4137, Evidence/Property Custody Document (EPCD), Document Number (DN) 78-10 to describe the evidence, and signed it over to the evidence custodian, Mr. Garon Young. I do not have any reason to believe that the evidence suffered damage or contamination. I did not touch this evidence again. **Prosecution Exhibit (PE) 97 for Identification** is DN 78-10, the DVD containing the DoS server logs.



ASHDEN FEIN
MAJ, JA
Trial Counsel



THOMAS F. HURLEY
MAJ, JA
Military Defense Counsel



BRADLEY E. MANNING
PFC, USA
Accused